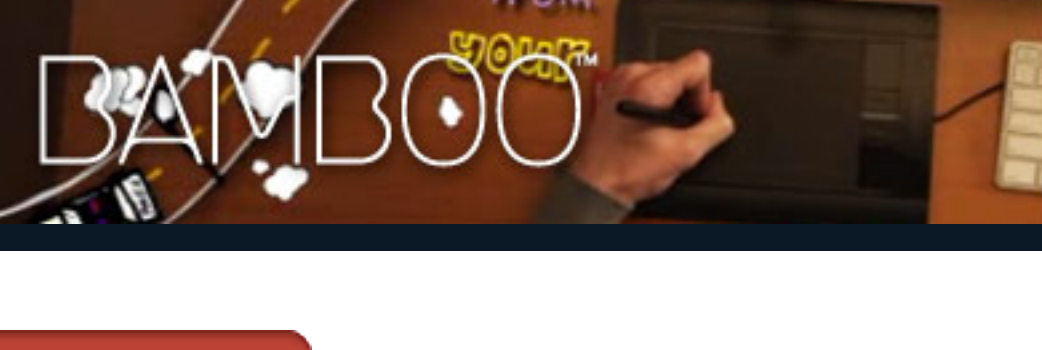


Macworld Magazine
Subscribe & Get a Bonus CD
Customer Service

38 APPS



Make It Yours

iPhone Central

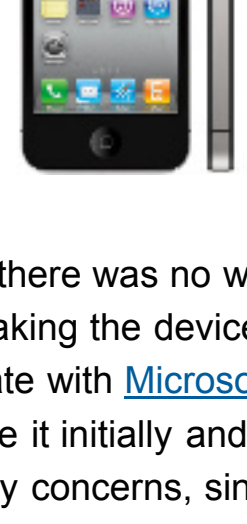
All about the iPhone, iPod touch, and App Store from the Apple experts

0 Comments | +3 Recommendations | |

Managing and securing iOS 4 devices at work

Posted on Aug 17, 2010 3:00 pm by [Ryan Faas](#), [Computerworld](#)

Editor's Note: This story is excerpted from [Computerworld](#). For more Mac coverage, visit [Computerworld's Macintosh Knowledge Center](#).



Apple's [iPhone](#) has always had something of an image problem in the workplace, which isn't surprising given that Apple has always marketed its smartphone more to consumers than to the business world.



16GB iPhone 4
Complete Coverage »

4.0 out of 5 Mice
Jun 28, 2010

Best current price: \$299.00

In fact, when the iPhone debuted in 2007, there was no way to put third-party apps on one without jailbreaking the device, it didn't support 3G data networks, it didn't integrate with [Microsoft's](#) Exchange, and you had to use iTunes to activate it initially and back up or sync data later on. Plus, there were security concerns, since there was no way to require a passcode, encrypt business data or remotely wipe an iPhone if it was lost or stolen.

A lot has changed for the iPhone, its operating system and the [smartphone](#) industry as a whole in three years. For people who want to use the iPhone at work and the IT departments that support them, the changes have been good. In fact, some of the major updates in each new iteration of the iPhone operating system (now called iOS) were the ones that made it [easier to manage](#) and secure Apple's mobile platform.

With each passing summer, [Apple](#) has polished the business and [enterprise](#) features of iOS. It has added Exchange support, support for remote wipe, security and [configuration policies](#) (either through Exchange or with configuration profiles that can be loaded onto each device), VPN options and encryption—both whole-device encryption on the iPhone 3GS and targeted app data encryption in iOS 4.

While each of the changes was an improvement, it wasn't until this year's [arrival of iOS 4](#)—and the [iPhone 4 itself](#)—in June that Apple introduced a new mobile device management (MDM) service that companies could use. As a result, businesses finally got something sorely needed for enterprise iPhone adoption to make sense: the ability to more easily deploy, manage and monitor iPhones used by employees — a capability that has long made Research In Motion's BlackBerry one of the most trusted mobile platforms.

Note: Although iOS 4 has been rolled out for the iPhone, the iPad won't get the operating system upgrade until this fall.

Third-party vendors are part of the equation

One surprising thing about how Apple rolled out MDM is that the company largely left implementing it via a server up to other companies. Considering Apple's penchant for secrecy about upcoming products and its tight control over the App Store, this move seemed odd of character. Most people, myself included, figured Apple would offer a robust over-the-air device management solution. And we expected Apple to take a page from RIM's BlackBerry Enterprise Server and ship something as part of its own Mac OS X Server platform. (That could still happen in the next major OS X Server release.)

Whether or not Apple comes out with its own management server, there are advantages for companies looking to support iOS devices in a secure and managed way. The most obvious one is competition. With seven different options either already on the market or slated to be available by year's end, companies can choose the one that works best for them. Although many of the core management features of iOS 4 and the MDM service offered by each vendor are essentially the same, there's still plenty of differentiation among them.

In some cases, the main difference may simply be the management interface. Or it can mean different levels of integration with other technologies such as Active Directory. Other variables run the gamut from the type and format of reports about mobile device use to system requirements (one option is completely Mac-based), cost, existing relationships with providers and the number of non-iOS platforms each can manage.

Standardizing on a mobile platform is tough

Having a standard computing platform is a relatively simple task for most businesses, partly because there's a limited set of choices: some variation of Windows or Mac OS X. (Yes, [Linux](#) and Unix are options, but they typically aren't chosen for people outside of IT.)

Getting hardware is also easy, since most purchases are made in bulk and typically from a single vendor. If you're a Mac shop, you're buying Apple hardware; if you opt for Windows, hardware choices are plentiful.

That kind of standardization doesn't work as well for smartphones and tablets. Even if your company pays for a smartphone for each employee, IT shops are still apt to encounter problems. Being tied to a single carrier may not be a good choice for all workplaces; different phone models may sport different features (and potentially different management capabilities); phones might only run certain versions of operating systems or offer different sets of bundled or available apps; and there may be varying levels of integration with other systems like VPN, mail servers and intranets.

When workers bring their personal devices to work—as more of us are doing these days—there's even more potential for problems. IT shops may not even know what devices employees are using, or for what purpose—to say nothing about how secure they are.

A few years ago, companies could afford to buy mobile hardware for their employees. That's no longer true, and many organizations are embracing the concept of bring-your-own-hardware-to-work. That saves a lot of money, since there's no hardware to buy and no monthly cell phone bill (for the company). But then you have to manage and secure those devices—or try to dictate what your workers use. (Good luck with that one.)

The most important advantage to Apple's approach to MDM is that all but one of the third-party companies that have announced or released management servers offer support for platforms beyond iOS. Two of them, Absolute Manage and AirWatch, offer management capabilities for devices other than smartphones or tablets.

Apple would be hard-pressed to develop its own such multiplatform system, as would any smartphone manufacturer. Of course, the specific mix of supported platforms varies with each product, as does the extent of supported features. But that's the advantage of competition: You should be able to get the one that best meets corporate needs.

Understanding configuration profiles in iOS

A central component to managing mobile devices involves what Apple calls configuration profiles. These are XML lists of different configuration features and optional restrictions that automatically configure an iOS device.

A single configuration file can contain all of the available settings for an iPhone—complete with user credentials for various network resources—or it may contain just a single value that's not user-specific, such as the details for accessing your mail server, VPN or wireless network. If you put in a server or network-related configuration without specific user credentials, the user will be asked to authenticate the first time they access the resource.

You can assign as many separate granular profiles as you like to any or all phones and they'll all be enforced. This is helpful if you need to assign configuration data based on job function or department.

The most important features you can set using configuration profiles involve security: requiring a passcode, setting passcode restrictions and forcing employees to use long and complex passcodes. You can also specify how quickly a device locks when not in use and how many failed attempts to unlock it with a passcode are allowed before the device automatically wipes data.

Another security-related option allows you to disable an iPhone's built-in camera(s). Since it is common for employees to ban camera-enabled devices to avoid sensitive information from leaking, this is an important option in many organizations.

Beyond the security options, there are a number of ways to customize an iOS device for use with your company's network and resources. You can preconfigure access to Wi-Fi networks, VPN and e-mail servers. You can also pre-populate bookmarks for the mobile Safari browser to ensure that users can easily access internal (or external) Web-based resources. You can even specify Web pages or Web apps to appear as icons on a devices home screen for easier access.

In short, you can do a lot with configuration profiles to lock down an iPhone.

For more details about configuration profiles, check out Apple's documentation of the iPhone Configuration Utility. This is the free tool (available for Mac and Windows) that Apple developed for creating and testing configuration profiles. Apple also offers information about various management and deployment scenarios as well as overviews for iOS 4 business integration.

In addition to setting configurations through profiles, the MDM service allows you to query any managed device for more than 20 different pieces of data (including device- and carrier-specific details, as well as usage and verification that security policies are being enforced).

Beyond setting configuration profiles and querying forces, the MDM service allows you to take certain actions on managed devices. You can, for instance, force the device to lock and/or wipe all data. And you can temporarily remove a passcode (in case a remote user has forgotten it). If a passcode is required, the user will be required to create a new one.

You can also install or update configuration profiles as well as installed apps and enterprise application provisioning profiles and in-house apps. All this can be done in the background without user intervention, allowing you to make sure that software, configuration and security policies are in place.

(See below for a full list of the available management and monitoring capabilities of iOS 4.)

Enrolling iOS devices for management

Apple made the process of setting up device management pretty simple using SCEP. A user is instructed to visit a secure Web site and authenticate with his or her user account (typically an Active Directory account or some other LDAP-based directory service). This allows the iPhone to generate a certificate enrollment request and then an identity certificate for the device.

Using that identity certificate and the user's credentials to establish a secure connection, the device then processes the list of assigned configurations and presents them to the user. When the user agrees to the configurations, the device will download and install the related profiles and can be fully managed.

Management server options

Now that we've covered the what and the how of enterprise management, here's the list of vendors and the expected ship dates for their products:

- Absolute Manage: Expected availability in the third quarter of this year.
- Afaria by Sybase: iOS 4 beta program now in progress, with availability also expected in the third quarter.
- AirWatch: Availability listed as summer 2010.
- Good for Enterprise: Now available.
- MobileIron: Now available, and offering discounts to existing Good customers.
- Tangoe Mobile Device Manager: Now available.
- Tarmac by Equinix: Now available.

Note: Equinix is known for media and networking tools for Mac OS X and iOS. Tarmac is its first step into the realm of device management and is an iOS-specific solution. It lists a Mac as part of its system requirements, and overall it might be better for small and midsize organizations — particularly those that have a strong Apple presence.

Management and monitoring options for iOS devices

When building configurations, you can specify details about the following: Exchange or POP/IMAP mail servers; VPN configurations; Wi-Fi networks (including hidden networks and networks requiring a passcode or radius authentication); LDAP directories for contacts, access to a CalDAV and/or CardDAV server, public or private calendars that support iCal (.ics) subscriptions; carrier (APN) settings; digital certificates; and Web clips.

You can also mandate a variety of security policies, such as requiring an unlock passcode; allowing a simple passcode or requiring an alphanumeric passcode with a special character; setting how long a passcode can be used; specifying the length of time before automatic screen locking takes place; setting the number of failed passcode attempts allowed before the device is wiped automatically; requiring that the backup profiles when syncing to iTunes be encrypted; and indicating whether users can remove configuration profiles.

When it comes to locking down an iOS device, you can restrict access to the following: app installation, the camera, screen captures, automatic mail sync while roaming, voice dialing while the device is locked, in-app purchases, items tagged by iTunes as explicit and access to the security settings for the mobile Safari [browser](#). You can also keep users from launching Safari, YouTube, the iTunes Store and the App Store.

The goal is as simple as your company wants as needed to ensure that the device is as locked down as you require.

In addition to device management, MDM is a service that relies on Apple's push notification system to receive queries and instructions from a management server to interact with any iOS 4 device in the background. That it runs as an always-on background process is the reason third-party vendors couldn't create such a solution on their own.

You can build queries for a single device or multiple devices that encompass the following areas: unique device identifier (a value unique to each iOS device); the device name; iOS version; model name and hardware version; serial number; total storage capacity and available free space; IMEI number; the modern firmware version; SIM card ICCID; MAC addresses for both the Wi-Fi and Bluetooth receivers; current carrier (home carrier or roaming); the carrier identified by the installed SIM card as the primary carrier; the version of the carrier settings (APN) data; phone number; whether data roaming is allowed; the installed profiles; installed security certificates and their expiration dates; enforced restrictions; hardware encryption capability; whether a passcode is set; installed applications (including app identifier, name, version, and size); and any application provisioning profiles and their expiration dates—something that's required for internal corporate iPhone apps distributed outside of the App Store.

Some final thoughts

It's still unclear whether iOS 4 will truly end the belief that the iPhone (and [iPad](#)) platform is more about personal entertainment than workplace functionality. It's also hard to know for which smartphone and tablet platforms will have the staying power to dominate the market — though I wouldn't bet against Apple. For now, it seems clear that workers and businesses will have a wide variety of choices over the next few years, with Apple being just one of many players trying to get their feet in the enterprise door.

Being able to effectively support and manage multiple platforms is crucial for any organization that wants an effective mobile strategy. For iOS 4 devices, and others, these tools offer ways to make the coming diversification easier to manage and secure. And while they certainly don't ensure that Apple's devices will be welcomed by IT shops, they do make them increasingly viable options for companies in the years ahead.

[Ryan Faas is a freelance writer and technology consultant specializing in Mac and multiplatform network issues. He has been a Computerworld columnist since 2003 and is a frequent contributor to Peachpit.com. Ryan was also the co-author of O'Reilly's Essential Mac OS X Panther Server Administration.]

See more like this: [iOS](#), [iPhone](#), [iPhone 4](#), [users enterprise](#)

Recommend? | | | |

ADS BY GOOGLE

[Apple Mac mini bei Gravio](#)
Apple Mac mini kaufen und mit dem Gravis MacPack bis zu 295 € sparen!
[www.gravis.de/Mac_mini](#)

[Fernwartung von/iur Macs](#)
Macs sicher und schnell fernwarten. Kostenlos Testen!
[www.TeamViewer.com/Mac](#)

[Earbuds Fall Out?](#)
BudFits - The most secure way to wear earbuds. Only \$9, Ship Free.
[www.BudFits.com](#)

"Managing and securing iOS 4 devices at work" Comments

[View and post a comment »](#)

[Sign in](#) to post a comment. New to Macworld Comments? [Register here](#).

GET THE MOST OUT OF YOUR NEW MAC
New Macworld Superguides

YOUR GUIDE TO 100,000+ IPHONE APPS
Macworld's App Gems app

Make Your Dreams Come True!

Enter for a chance to win \$25,000 or your choice of other great prizes in the Dream Come True Sweepstakes brought to you by Macworld.
[Enter now »](#)

About iPhone Central

Get the latest news, reviews, and opinion about Apple's groundbreaking iPhone from the Apple experts at Macworld.

Tip Us Off: [iphone \[at\] macworld \[dot\] com](#) [Email: 1-415-520-9761](#)

[Subscribe/RSS](#)

[Subscribe to our weekly iPhone newsletter](#)

Want more information? Be sure to check out our complete iPhone coverage.

All about the iPad
Everything about Apple's new device

[Review: Apple iPad Wi-Fi + 3G](#)

[Review: Apple iPad Wi-Fi](#)

[The iPad up close](#)

[Updated FAQ: What you need to know](#)

[5 iPad folio-style cases](#)

Macworld iPod Touch & iPhone App Review Essential Collections [View all »](#)

Friend or Foe?
Keep your friends close and your enemies closer. But keep these mobile apps close at hand at all times.

[Frienemies](#) Games | Not yet rated

[Words With Friends HD](#) Games | 4.5 out of 5 Mice

[My Enemies](#) Photography | Not yet rated

[Get My Friends](#) Social Networking | Not yet rated

[Insult - How To Make Enemies and Alienate The People](#) Entertainment | Not yet rated

[View all "Friend or Foe?" apps »](#)

[VIEW ALL 248772 IPOD TOUCH & IPHONE APP REVIEWS »](#)

ADS BY GOOGLE

[Mac Remote Access](#)
Total Remote Access w/ No Set-up. Works through Firewalls, Try Today!
[LogMeIn.com/LogMeIn_for_Mac](#)

[Photo processing for OS X](#)
Vintage styles, lomo, tiltshift, sepia, frames. Get free trial now!
[corner-a.com/photostyle](#)

[OS X Data Recovery SW](#)
Recover Lost Data from Hard Drives Free Demo, Fast Recovery, Try Now
[macintosh-data-recovery.com/recover](#)

[Centrify Active Directory](#)
Control Cross-Platform User Access w/ Active Directory. Sign Up Now
[www.Centrify.com/FreeWhitePaper](#)

[Faire Kredite ab 3.45%](#)
Kredite jetzt individuell & schnell abfragen - Mit Bestzins-Garantie!
[www.Kredit-Testsieger.Geld.de](#)

Home

MACWORLD CHANNELS

Mac | iPhone & iPad | Digital Photo | iPod & Entertainment

Create | Business Center | Macworld App Guide

NEWS, REVIEWS, HELP & TIPS, AND PRODUCT INFORMATION

Audio | Home Theater | Printers | Software & Security

Blu-Ray | Input Devices | Projectors | Web Browsers

Camera Accessories | iPods | Scanners | Education

Camcorders | Macs | Smartphones | E-Mail & Internet

Desktop Macs | Mac Accessories | SLRs | Games

E-Readers | MacBooks | Storage | Graphics & 3-D

GPS | Servers | Tablets | Music and Audio

Hard Drives | Monitors | Video Players | Video Software

Headphones | Networking & Wireless | Web Services | Networking Utilities

HDTV | Optical Drives | Web Productivity Apps | Office Software

Home and Car Audio | Phone accessories | Point-and-Shoot | Operating Systems

Photography Software

Programming

Publishing Software

Print Publishing

Web Publishing

Utilities

Try Macworld Risk Free

And get a BONUS CD-ROM

Name City

Address 1 State Zip

Address 2 E-mail (optional)

Canadian Residents | Foreign Residents | Gift Subscriptions | Customer Service | Privacy Policy